



# Irides Security Policy

# Irides Security Policy

The following is a list of standard Irides security policies and procedures.

## System Access Control

### Minimum Password Length

The length of passwords must always be checked automatically at the time that users construct or select them. All passwords must have at least eight (8) characters.

### Passwords Require Change Periodically

User-chosen passwords will require changing at least every 90 days. Several warnings will be presented to the user to make the required change at least 1 week before the 90 days are up. If the user fails to make the required change within the 90 days, the user account will be de-activated.

### Difficult-To-Guess Passwords Required

All user-chosen passwords for computers and networks must be difficult to guess. Words in a dictionary, derivatives of user-IDs, and common character sequences such as "123456" should not be employed. Likewise, personal details such as spouse's name, automobile license plate, social security number, and birthday must not be used unless accompanied by additional unrelated characters. User-chosen passwords must also not be any part of speech. For example, proper names, geographical locations, common acronyms, and slang must not be employed.

### Cyclical Passwords Prohibited

Users are prohibited from constructing fixed passwords by combining a set of characters that do not change, with a set of characters that predictably change. In these prohibited passwords, characters which change are typically based on the month, a department, a project, or some other easily-guessed factor. For example, users must not employ passwords like "X34JAN" in January, "X34FEB" in February, etc.

### User-Chosen Passwords Must Not Be Reused

Users must not construct passwords that are identical or substantially similar to passwords that they had previously employed.

### Passwords Never In Readable Form When Outside Workstations

Fixed passwords must never be in readable form outside a personal computer or workstation (e.g. sticky notes).

### Password Guessing Lockout Requires Help Desk

#### Password Reset

Each user of the Irides computer systems that employ fixed passwords at log-on time will be given a limited number of attempts to enter a correct password. If a user has incorrectly entered a password three consecutive times, the linked user-ID will be deactivated until Irides staff authenticates the user's identity and then resets the password.

### Prevention Of Password Retrieval

Computer and communication systems must be designed, tested, and controlled so as to prevent both the retrieval of, and unauthorized use of stored passwords, whether the passwords appear in encrypted or unencrypted form.

### Password Sharing Prohibition

Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions that the other party takes with the password. If a password is provided to a Irides IT support representative in order to help diagnose a specific user issue, that user should change their password immediately after the issue is resolved.

### Users Responsible For All Activities Involving Personal User-IDs

Users are responsible for all activity performed with their personal user-IDs. User-IDs may not be utilized by anyone but the individuals to whom they have been issued. Users must not allow others to perform any activity with their user-IDs. Similarly, users are forbidden from performing any activity with IDs belonging to other users (excepting anonymous user-IDs like "guest").

### Removal of User-ID for Termination or Job Change

Clients should notify Irides immediately upon termination or a job change of one of its users such that they will no longer require system's access. Upon receipt of notification, Irides will

Irides, LLC

immediately deactivate and remove the User ID from the system.

### **Irides Password Management**

All Irides controlled passwords (e.g. server root passwords, network device passwords, client access passwords) will be stored encrypted and not be produced in printed format. Passwords will never be shared between Irides employees and/or clients in clear text format. PGP is the general standard Irides uses to encrypt data and pass data securely between both employees and clients.

### **Desktop Lockout Settings**

All clients requiring desktop support services from Irides are requested to implement a desktop timeout feature (screen saver) with password control set to a minimum of 30 minutes. This policy is provided to reduce the possibility of unauthorized attempts made to the client's specific desktop and connected networked infrastructure.

## **Privilege Control**

### **Third Party Access To Irides Systems**

Before any third party is given access to Irides computer systems, written agreement to abide by Irides Rules and Regulations must have been signed by a responsible manager at the third party organization.

### **Support For Special Privileged Type Of Users**

All multi-user computer and network systems must support a special type of user-ID which has broadly-defined system privileges. This user-ID will in turn enable authorized individuals to change the security state of systems. The number of privileged user-IDs must be strictly limited to those individuals who absolutely must have such privileges for authorized business purposes.

### **Restriction Of Special System Privileges**

Special system privileges, such as the ability to examine the files of other users, must be restricted to those directly responsible for system management and/or security. File access control permissions for all Irides computer systems must be set to a default which blocks access by unauthorized users. Beyond that which they need to do their jobs, computer operations, hardware and systems support staff must not be given access to--nor permitted to modify--production data, production programs, or the operating system.

### **Unbecoming Conduct And The Revocation Of Access Privileges**

Irides reserves the right to revoke the privileges of any user at any time. Conduct that interferes with the normal and proper operation of Irides information systems, which adversely affects the ability of others to use these information systems, or which is harmful or offensive to others will not be permitted.

### **Termination Of User Processes Or Sessions And Removal Of User Files**

Irides systems administration staff may alter the priority of, or terminate the execution of, any user process which it believes is consuming excessive system resources, significantly degrading system response time, or if this usage is deemed to be in violation of security policies.

### **Maintenance Of Master User-ID And Privilege Database**

So that their privileges may be expediently revoked on short notice, records reflecting all the computer systems on which users have user-IDs must be kept up-to-date.

## **Monitoring and Logging**

### **Inclusion Of Security Relevant Events In System Logs**

Computer systems handling sensitive, valuable, or critical information should securely log all significant security relevant events. Examples of security relevant events include but are not limited to: password guessing attempts, attempts to use privileges that have not been authorized, modifications to production application software, and modifications to system software.

### **Computer System Logs Must Support Audits**

Logs of computer security relevant events must provide sufficient data to support comprehensive audits of the effectiveness of, and compliance with security measures.

## **Intellectual Property Rights**

### **Information As An Important Irides Asset**

Accurate, timely, relevant, and properly protected information is absolutely essential to Irides and its clients. To ensure that information is properly handled, all accesses to, uses of, and processing of Irides internal or client information must be consistent with Irides information systems related policies and standards.

### **Tools Used To Break Systems Security Prohibited**

Unless specifically authorized by Irides no person shall use hardware or software tools that could be employed to evaluate or compromise information systems security. Examples of such tools include but are not limited to those that defeat software copy protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files.

### **Valid Client Software Licenses**

Irides staff are not permitted to install client software without valid software licensing provided by the client.

## **Data Privacy and Confidentiality**

### **Notification Of Suspected Loss Or Disclosure Of Sensitive Information**

If sensitive information is lost, is disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, its owner and Irides Management should be notified immediately.

## **Data Integrity**

### **Right To Remove (Offensive) Material Without Warning**

Irides Management retains the right to remove from its information systems any material it views as (offensive) or potentially illegal.

### **No Responsibility For Monitoring Content Of Information Systems**

Irides Management reserves the right to remove any message, file, database, graphic, or other material from its information systems. At the same time, Irides Management has no obligation to monitor the information content resident on or flowing through its information systems.

## **Establishment Of Access Paths And Systems**

### **Security Requirements For Network-Connected Third Party Systems**

As a condition of gaining access to the Irides computer network, every third party must secure its own connected systems in a manner consistent with Irides requirements. Irides reserves the right to audit the security measures in effect on these connected systems. Irides also reserves the right to immediately terminate

network connections with any third party systems not meeting such requirements.

### **Standards Of Common Carriers Do Not Apply**

The networking services provided by Irides are provided on a contractual carrier basis, not those of a common carrier. As the operator of a private network, Irides has a right to make policies regarding the use of its network systems without being held to the standards of common carriers.

## **Encryption**

### **Standard Encryption Algorithm & Implementation**

If encryption is used, government-approved standard algorithms (such as the Data Encryption Standard or DES) and standard implementations (such as cipher-block chaining) must be employed.

### **Disclosure Of Encryption Keys Requires Special Approval**

Encryption keys are a most sensitive type of information, and access to such keys must be strictly limited to those who have a need-to-know. Unless the approval of Irides is obtained, encryption keys must not be revealed to consultants, contractors, or other third parties.

### **Time Period For Protection Of Encryption Keys Used For Confidentiality**

The secrecy of any encryption key used for confidentiality purposes (e.g., for data encryption or as a seed to an access control system) must be maintained until all of the protected information is no longer considered confidential.

### **Never Automatically Backup Private Key Used For Digital Certificates**

Users must not allow automatic backup systems to make a copy of the readable version of their private key used for digital signatures and digital certificates. Automatic backups could allow unauthorized transactions to be generated in the involved users' names. These backups are prevented by keeping private keys in smart cards or otherwise in encrypted form.

### **Prevention Of Unauthorized Disclosure Of Encryption Keys**

Encryption keys must be prevented from unauthorized disclosure via technical controls such as encryption under a separate key and use of tamper-resistant hardware.

## **Explicit Assignment Of Encryption Key Management Functions**

Whenever encryption is used to protect sensitive data, the relevant owner(s) of the data must explicitly assign responsibility for encryption key management.

## **Internet and Remote Dial Up Connections**

### **Digital Certificate For All Irides Internet Web And Commerce Sites**

A current digital certificate is recommended for both Irides and client Internet servers handling confidential information.

## **Administrative Security**

### **Required Reporting of Information Security Incidents**

All suspected Information Security incidents must be reported immediately to Irides Management.

### **Centralized Reporting Of Information Security Problems**

Information Security is the inability of unauthorized third parties to access any documents, data or other information stored or otherwise normally available to authorized parties on Irides network or any Irides infrastructure components. All known vulnerabilities - in addition to all suspected or known violations - must be communicated in an expeditious and confidential manner to Irides Management. Unauthorized disclosures of Irides information must additionally be reported to the involved information owners. Reporting security violations, problems, or vulnerabilities to any party outside Irides (except external auditors) without the prior written approval of the Irides Legal Department is strictly prohibited. No external reporting of any Information Security violation or problem may occur without consent of Irides Management.

### **Required Investigation Following Computer Crimes**

Whenever evidence clearly shows that Irides has been victimized by a computer or communications crime, a thorough investigation must be performed. This investigation must provide sufficient information so that Irides Management can take steps to ensure that: (1) such incidents will not be likely to take place again, and (2) effective security measures have been reestablished.

### **Information Ownership And Management's Responsibilities**

All production information possessed by or used by a particular client must have a designated owner. Owners must determine

appropriate sensitivity classifications as well as criticality ratings. Owners must also make decisions about who will be permitted to access the information, and the uses to which this information will be put. Owners must additionally take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of information. Designated owner lists are to be provided to Irides Management and reviewed on a no less than annual basis.

## **Outsourcing and Third Party Contracts**

### **Agreements With Third Parties Which Handle Irides Information**

All agreements dealing with the handling of Irides information by third parties where the third party has direct access to Irides information must include a special clause. This clause must allow Irides to audit the controls used for these information-handling activities, and to specify the ways in which Irides information will be protected.

### **Termination Of Outsourcing Contracts For Security Violations**

All information-systems-related outsourcing contracts must be reviewed and approved by Irides Management. It is Irides Management's responsibility to make sure that these contracts sufficiently define information security responsibilities, as well as how to respond to a variety of potential security problems. It is also Irides Management's responsibility to make sure that all such contracts allow Irides Management to terminate the contract for cause if it can be shown that the outsourcing firm does not abide by the information security terms of the contract.